

# Technisches Datenblatt

Stand 01/2022 ▪ Änderungen und Irrtümer vorbehalten.

## GnuPG VS-Desktop®

GnuPG VS-Desktop® unterstützt 32- und 64bit-Windows-Systeme ab Version 7 oder neuer. Das GpgOL Plug-in ist kompatibel mit Outlook 2010, 2013, 2016 und 2019 und unterstützt Mailtransport per SMTP/IMAP und Exchange Server ab 2010.

GnuPG VS-Desktop®	
Datenverschlüsselung	OpenPGP   S/MIME   Symmetrisch
Mailverschlüsselung	PGP/MIME   S/MIME
Autom. Schlüsselabruf	OpenPGP über Web Key Directory   S/MIME über Zertifikatsserver
Vertrauensmodelle	Direkt   WoT (Web of Trust)   TOFU+PGP (Trust on first Use)
Authenticated Encryption	Nur in OpenPGP
VS-NfD (EU-RESTRICTED)	S/MIME mit Smartcard   OpenPGP und S/MIME ohne Smartcard <sup>(1)</sup>
VS-V (EU-CONFIDENTIAL)	Nach Bewertung durch das BSI
Compliance	de-vs   OpenPGP   RFC4880bis   PGP6   PGP7   PGP8   RFC2440
Unterstützte Smartcards	OpenPGP   NetKey   Yubikey   NitroKey   GnuK   PKCS#15   SC-HSM
ECC-Unterstützung für OpenPGP	Brainpool   NIST-P   Curve25519   Bitcoin
Zufallsgeneratoren	CSPRNG (DRG.3) mit Jitter-RNG <sup>(2)</sup>   RDRAND   Padlock
Algorithmen	AES   Twofish   Camellia   SHA-256   SHA-512   RSA (bis 8192)   EdDSA   ECDH   ECDSA   DSA (deterministisch RFC6979)
Webbrowser (PKCS#11)	Hardware- und Software-Token (Firefox, Thunderbird etc.)
Webbrowser (WebMail)	Firefox   Chrome (z.B. mit Mailvelope)
Authentifizierung	Hardware- und Software-Token (SSH und PAM)

GpgOL Outlook Plug-in	
Adressbuch-Integration	Festlegen und Verteilen der Schlüssel über das Adressbuch
Autocrypt-Unterstützung	Optional lesend. Inkl. verschlüsseltem Betreff
EFAIL-Schutz	Authenticated Encryption für OpenPGP   Absicherung für S/MIME
Nachrichtenleiste	Direktes Entschlüsseln ohne Interaktion
Inline-Editoren	Schnelles Antworten und Weiterleiten
Kompatibilitätsmodi	PGP/Inline
Phishing-Schutz	Über unterschiedliche Vertrauensstufen
Server	Microsoft Exchange (ab Version 2010)   IMAP
Verschlüsselte Entwürfe	OpenPGP   S/MIME

<sup>(1)</sup> Voraussetzung hierfür sind zusätzliche Schutzmaßnahmen, siehe VSA-BSI-10573.

<sup>(2)</sup> Kein Einsatz des Windows-Zufallsgenerators.